

Kaoru Uchida
Filed 2/5/01
Q62922
10f1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

JCS86 U.S. PTO
09/775617
02/05/01

出 願 年 月 日

Date of Application:

2000年 2月 3日

出 願 番 号

Application Number:

特願2000-025816

出 願 人

Applicant (s):

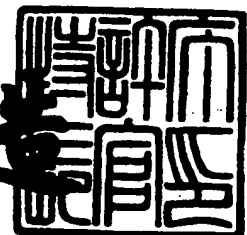
日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月10日

特許庁長官
Commissioner,
Patent Office

及川耕造



【書類名】 特許願

【整理番号】 33509686

【提出日】 平成12年 2月 3日

【あて先】 特許庁長官殿

【国際特許分類】 G06K 9/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 内田 薫

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088812

 【弁理士】

 【氏名又は名称】 ▲柳▼川 信

【手数料の表示】

 【予納台帳番号】 030982

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 バイオメトリクス入力装置及びバイオメトリクス照合装置

【特許請求の範囲】

【請求項 1】 個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを有することを特徴とするバイオメトリクス入力装置。

【請求項 2】 前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項 1 記載のバイオメトリクス入力装置。

【請求項 3】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 1 または請求項 2 記載のバイオメトリクス入力装置。

【請求項 4】 個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを有することを特徴とするバイオメトリクス入力装置。

【請求項 5】 前記センサ手段と前記秘密情報保持手段及び前記バイオメトリクス暗号化手段とを不可分な部分として構成するようにしたことを特徴とする請求項 4 記載のバイオメトリクス入力装置。

【請求項 6】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 4 または請求項 5 記載のバイオメトリクス入力装置。

【請求項 7】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段

とを有することを特徴とするバイオメトリクス照合装置。

【請求項 8】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 7 記載のバイオメトリクス照合装置。

【請求項 9】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項 1 0】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 9 記載のバイオメトリクス照合装置。

【請求項 1 1】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項 1 2】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 1 1 記載のバイオメトリクス照合装置。

【請求項 1 3】 バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを有することを特徴とするバイオメトリクス照合装置。

【請求項 1 4】 前記バイオメトリクスとして指紋を用いるようにしたことを特徴とする請求項 1 3 記載のバイオメトリクス照合装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はバイオメトリクス入力装置及びバイオメトリクス照合装置に関し、特に情報セキュリティ等におけるユーザ確認、個人識別のためのバイオメトリクス入力装置及びバイオメトリクス照合装置に関する。

【0002】

【従来の技術】

情報の電子化やネットワークを通じての情報サービスにおいて、データの盗聴・改竄や「なりすまし」といった不正・犯罪に対抗するセキュリティの確保のためには、情報にアクセスする人間が正当な権限を持つユーザであるか、または価値の交換の相手が自分の望むユーザであるかを確認するための本人確認の実現が必須の条件となる。

【0003】

現在、本人確認には磁気カードやパスワードが利用されているが、例えばカードをなくしたり、パスワードを忘れてしまうと本人でも使えないという不便さがあるのはもちろん、いずれの場合も盗難・偽造や盗み見・推量によって容易に他人がなりすませるといった問題点がある。

【0004】

そこで、これらの問題点を解決するバイオメトリクスが用いられる。バイオメトリクスとは指紋のような個人に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は「万人不同」・「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【0005】

バイオメトリクスによって個人を認証するシステムは基本的に、ユーザが提示したバイオメトリクスをシステム側で取得する「バイオメトリクス入力装置」と、入力されたデータを処理し照合に用いる特徴を求める「特徴抽出部」と、予め求めて記憶しておく正規ユーザについての登録データ（「テンプレート」）と、

登録データと入力データ（の特徴同士）とを比較して同一人物であるか否かを決定する「照合・判定部」とから構成されている。

【 0 0 0 6 】

照合の結果、特徴が十分類似し、バイオメトリクスの提示者が登録ユーザであると判定されれば、認証成功ということで、認証要求者は要求するサービスを受けられる。以下、バイオメトリクスの例として指紋を挙げて説明する。

【 0 0 0 7 】

指紋の入力装置としては従来、光学方式、特に高コントラストな画像を得るためにプリズムでの全反射を利用する方法のみが用いられてきている。これはLED (Light Emitting Diode) 光源で発した光をプリズムに当ててからCCD (Charge Coupled Device) のような受光素子で受け、プリズムの反射面に置いた指の凹凸を反射率の違いに反映させ、デジタル画像化するというものである。

【 0 0 0 8 】

また近年は、光学方式以外のセンシングを可能とする素子として、半導体チップの表面に直接接触させた指紋からその凹凸をセンスする、例えば静電容量方式のもの、温度や電界の差を検知する方式のもの等も実用化されつつある。

【 0 0 0 9 】

【発明が解決しようとする課題】

指紋照合処理の実現方法としては、入力装置が指紋の入力だけを行い、識別処理が接続されたPC（パーソナルコンピュータ）やネットワークで結ばれたサーバ等で行うという方法がとられることがある。

【 0 0 1 0 】

このように、指紋入力装置（スキャナ）と照合処理部とが分離している場合、入力装置（入力スキャナ、入力センサと呼ばれることもある）は指紋画像の入力を行い、それをケーブル等を通してPCに送り、そこで特徴抽出や照合・判定処理が実行される。

【 0 0 1 1 】

このような構成ではケーブルを付け替えて他の情報機器を結び、他の機会に入

手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するというセキュリティアタックがあり得る。この場合、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際には他人の指紋であったということが起こりうる。

【 0 0 1 2 】

そこで、本発明の目的は上記の問題点を解消し、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるバイオメトリクス入力装置及びバイオメトリクス照合装置を提供することにある。

【 0 0 1 3 】

【課題を解決するための手段】

本発明によるバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスを前記秘密情報保持手段に保持された暗号化鍵に基づいて暗号化して出力するバイオメトリクス暗号化手段とを備えている。

【 0 0 1 4 】

本発明による他のバイオメトリクス入力装置は、個人に固有の生体特徴であるバイオメトリクスをデジタル化するセンサ手段と、予め設定された秘密情報である暗号化鍵を保持する秘密情報保持手段と、前記センサ手段でデジタル化されたバイオメトリクスに前記秘密情報保持手段に保持された暗号化鍵を電子透かしとして埋め込む電子透かしエンコーダとを備えている。

【 0 0 1 5 】

本発明によるバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に前記保持手段に保持された前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【 0 0 1 6 】

本発明による他のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵に基づいて暗号化されたバイオメトリクスの入力時に別途入手した前記バイオメトリクス入力装置固有の暗号化鍵を用いて当該バイオメトリクスを復号化する復号化手段と、前記復号化手段で復号化された前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【 0 0 1 7 】

本発明による別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵を保持する保持手段と、前記暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と前記保持手段に保持された暗号化鍵とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【 0 0 1 8 】

本発明によるさらに別のバイオメトリクス照合装置は、バイオメトリクス入力装置毎に予め設定された秘密情報である暗号化鍵が電子透かしとして埋め込まれたバイオメトリクスの入力時に当該バイオメトリクスから前記暗号化鍵を取り出す手段と、その取り出された前記暗号化鍵と別途入手した前記バイオメトリクス入力装置固有の秘密情報とを比較して前記バイオメトリクス入力装置からの信号の正当性を判定する手段と、その判定結果を用いて前記バイオメトリクスの照合処理を行う照合処理手段とを備えている。

【 0 0 1 9 】

すなわち、本発明のバイオメトリクス入力装置は、入力装置で取得されるバイオメトリクスデータを入力装置固有の鍵で暗号化し、あるいは入力装置固有のデータを電子透かしとして埋め込むことで、照合装置側でバイオメトリクス入力装置の正当性を確認可能とする。

【 0 0 2 0 】

これによって、バイオメトリクス入力装置が改造・置換され、あるいは出力信

号が置換された場合にそれを検知することが可能となるので、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能となる。

【 0 0 2 1 】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図1は本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。図1においてはP C等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置1をケーブル等のローカルな接続によってP Cに接続し、P C上のソフトウェアで指紋照合部2が動作するようになっている。

【 0 0 2 2 】

指紋入力装置1には指紋センサ11が装備されており、指紋センサ11はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから画像暗号化部13に送る。暗号化鍵保持部12は一般ユーザ等に知られていない秘密情報としてその指紋入力装置1の個体固有の暗号化鍵を保持する。これは、例えば256ビットのビット列等である。

【 0 0 2 3 】

画像暗号化部13は暗号化鍵保持部12からその暗号化鍵を受取り、これを鍵として入力画像の暗号化処理を行う。この暗号化処理としては、DES (Data Encryption Standard) を例とするような共通秘密鍵方式の暗号化方法を用いることができるが、また一方、RSA方式を例とするような公開鍵方式（非対称暗号系）の暗号化方式を利用することも可能である。この場合、指紋入力装置1の持つ秘密鍵を暗号化に用いることになる。

【 0 0 2 4 】

また、用途によっては複雑な暗号化処理でなくても、入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を採用し、そのスクランブルを規定するルールを暗号化鍵として暗号化鍵保持部12に置くという方法も可能である。

【 0 0 2 5 】

一方、指紋入力装置 1 の構成法としては、指紋センサ 1 1、画像暗号化部 1 3、暗号化鍵保持部 1 2 を不可分な方法で構成することが望ましい。不可分であるとは、ここの部分の解読や改造を図る不当な第三者が、指紋センサ 1 1 から画像暗号化部 1 3 への内部信号、暗号化鍵保持部 1 2 から画像暗号化部 1 3 への内部信号を解読したり、それらの信号を外部からの信号で置き換えたり、あるいはそれぞれの構成要素の中身を解読したり改造したりできないように構成するということである。

【 0 0 2 6 】

この実現法としては、指紋センサ 1 1 の画像取得及びデジタル化を実行する半導体チップと同一チップ上に画像暗号化部 1 3 と暗号化鍵保持部 1 2 とを焼き込むという方法が有効である。一例としては、指紋センサ 1 1 の撮像部として C M O S (C o m p l e m e n t a r y M e t a l O x i d e S e m i c o n d u c t o r) のイメージャチップを利用し、その同一チップ上で暗号鍵の保持から暗号化演算までを行い、暗号化した結果を出力信号とするという実装があり得る。

【 0 0 2 7 】

あるいは、指紋センサ 1 1 の指紋画像取得方法として半導体センサによる静電容量方式の指紋センシングを利用し、その半導体センサ上に暗号鍵の保持から暗号化演算までを実装するということもできる。

【 0 0 2 8 】

指紋入力装置 1 とケーブル等のローカルな接続によって結ばれた指紋照合部 2 ではその内部の暗号化情報保持部 2 4 に、その指紋照合部 2 が接続して使用する指紋入力装置 1 の個体毎に固有な暗号化鍵を、その入力装置の識別子（装置 I D ）と対にして記憶しておき、現在接続されているはずの指紋入力装置 1 の装置 I D に対応する鍵を指紋復号化部 2 1 に渡す。画像復号化部 2 1 はその鍵を用い、指紋入力装置 1 から受取った信号を復号する。

【 0 0 2 9 】

この復号処理は指紋入力装置 1 の画像暗号化部 1 3 の処理内容に対応したものをを用い、正しく意味ある信号が復元できることをもって、指紋入力装置 1 及びそ

こから送られてくる信号の正当性を確認することとなる。

【0030】

例えば、画像暗号化部 1 3 が共通秘密鍵方式の暗号化方法を用いていれば、暗号化鍵保持部 1 2 に保持されたものと同一の鍵を用いた復号を行い、これで正しく復号できる場合には指紋入力装置 1 及びそこから送られてくる信号が正当なものであることを確認することができる。

【0031】

また、公開鍵方式（非対称暗号系）の暗号化方式であれば、指紋入力装置 1 の暗号化鍵保持部 1 2 に保持された秘密鍵に対応する公開鍵を用いて復号する。これで正しく復号できる場合には指紋入力装置 1 及びそこから送られてくる信号が正当なものであることを確認することができる。

【0032】

さらに、画像暗号化部 1 3 が入力画像のラインや画素毎にシフトしたり、入れ替えたりするスクランブル処理を用いた場合にも、暗号化鍵保持部 1 2 が持っているはずのスクランブルを規定するルールを鍵として暗号化情報保持部 2 4 に保持しておき、それを用いて対応する復号化を行う。これで正しく復号できる場合には指紋入力装置 1 及びそこから送られてくる信号が正当なものであることを確認することができる。

【0033】

指紋特徴抽出部 2 2 は画像復号化部 2 1 で復号された結果の画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル 2 6 は指紋照合に用いる指紋特徴情報をユーザ毎に保持している。指紋特徴照合部 2 3 は指紋特徴抽出部 2 2 で求められた指紋特徴とユーザ別指紋登録情報テーブル 2 6 に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部 2 5 に渡す。

【0034】

以上の指紋センサ 1 1、指紋特徴抽出部 2 2、指紋特徴照合部 2 3 を含む指紋照合装置の実現例としては、特開昭 5 6 - 2 4 6 7 5 号公報や特開平 4 - 3 3 0 6 5 号公報に記載された「指紋照合装置」がある。

【0035】

特開昭56-24675号公報に記載された「指紋照合装置」では、指紋等の照合に際して、指紋紋様を特徴付ける各特徴点の位置X、Y及び方向Dとともに各特徴点により固有に決定される局所座標系を複数の扇形領域に分割した近傍における最近傍点と上記特徴点との隆線数、すなわちリレーションを検査することによって、安定で、かつ精度の高い照合を可能にしている。

【0036】

また、特開平4-33065号公報に記載された「指紋照合装置」では、登録されている一つの指もしくは複数の指の全てと入力指紋との照合を行うことによって、暗証番号の盗難や忘却に関与しない、操作性が優れかつ信頼性の高い同定を可能としている。

【0037】

照合結果判定部25は指紋入力装置1から送られてくる信号の正当性と、指紋特徴照合部23で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部2は使用されているはずの指紋入力装置1に固有で秘密であるはずの鍵情報を暗号化情報保持部24のテーブルから探索し、それを用いて指紋入力装置1から送られる信号を復号し、それが正しく意味ある信号であるか否かを確認する。

【0038】

正しく意味ある信号とはすなわち、指紋入力装置1において指紋センサ11から出力された信号の形式に合致していることを意味し、これが合致している場合には指紋入力装置1が正当なもので、また指紋入力装置1からの信号は途中で改変されていないことが確認できたとして、指紋照合結果は信頼できるものであると判断する。

【0039】

一方、合致していない等、正しく復号できなかった場合には、それは指紋入力装置1が正当なものではないか、または指紋入力装置1からの信号が途中で改変されたことを意味するので、指紋照合結果は信頼できるものではないと判断することになる。

【0040】

図 2 は本発明の他の実施例による画像入力装置の構成を示すブロック図である。図 2 においては本発明の一実施例と同様に、PC 等においてユーザのログインを指紋で行う場合の構成の一例を示しており、指紋入力装置 3 をケーブル等のローカルな接続によって PC に接続し、PC 上のソフトウェアで指紋照合部 4 が動作する。

【0041】

指紋入力装置 3 には指紋センサ 11 が装備されており、指紋センサ 11 はユーザの指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから電子透かしエンコーダ 31 に送る。指紋入力装置秘密情報保持部 33 は一般ユーザ等に知られていない秘密情報としてその指紋入力装置 3 の個体固有の秘密情報を保持する。これは、例えばパスワードのような文字列等である。

【0042】

電子透かしエンコーダ 31 は指紋入力装置秘密情報保持部 33 からその秘密情報を受取り、電子透かしエンコード方式によってこれを入力画像に埋め込む。電子透かし技術とは次のような特徴を持つ。

【0043】

すなわち、(1) 透かしデータをコンテンツの中に、不可視の状態で埋め込むことができる、(2) 透かしを埋め込んだ者が必要な時に抽出することが可能である、(3) 透かしはコンテンツを加工しても残り、抽出が可能である、(4) コンテンツの利用価値を保ったまま第三者が電子透かしを除去するのは困難であるという特徴を持つ。(2) は暗号化技術におけるキーのような情報を設定し、キーを用いなければ情報が取り出せないような仕組みを設けることによって行われる。

【0044】

上記の電子透かし技術を使用することによって、コンテンツである指紋画像を劣化させることなく、電子透かしデータをその中に埋め込むことができ、そのデータを秘密に保つことができる。また、指紋画像を大幅に劣化させることなく、透かしデータを分離・削除・改変することもできない。電子透かし技術の実現法

の例としては、例えば特開平 8 - 2 4 1 4 0 3 号公報に記載の方法や特開平 1 0 - 2 2 4 7 9 3 3 号公報に記載の技術等がある。

【 0 0 4 5 】

特開平 8 - 2 4 1 4 0 3 号公報に記載の方法では、ウォーターマーク画像の画素を検査し、その値が指定された「透明」値でない画素のそれぞれについて、現画像の対応する画素を、その色度ではなく輝度を変更することによって修正することで、画像の内容を明瞭に見ることができるが、画像の無認可使用をおもいとどまらせる可視のマークをもたらすようにしている。

【 0 0 4 6 】

また、特開平 1 0 - 2 2 4 7 9 3 3 号公報に記載の技術では、電子透かしが挿入された M P E G (M o v i n g P i c t u r e E x p e r t a G r o u p) ストリームとともに、挿入された電子透かしデータも出力することで、挿入する電子透かしデータの管理を簡単にしている。

【 0 0 4 7 】

尚、上記の指紋入力装置 3 の構成法としては、本発明の一実施例と同様に、指紋センサ 1 1、指紋入力装置秘密情報保持部 3 3、電子透かしエンコーダ 3 1 を不可分な方法で構成することが望ましい。また、電子透かしエンコーダ 3 1 の出力信号はこのままユーザの指紋画像データが見える形で含むので、通信内容秘匿のために暗号部 3 2 において暗号化処理を行う。これは通常よく使われる D E S の秘密共通鍵方式等の暗号化方式でよく、以下に述べる復号部 4 1 と鍵情報を共用していればよい。

【 0 0 4 8 】

指紋入力装置 3 とケーブル等のローカルな接続によって結ばれた指紋照合部 4 においては、まず復号部 4 1 において通信内容秘匿のための暗号化を解き、電子透かしエンコーダ 3 1 の出力信号を復元する。その後、電子透かしデコーダ 4 2 において、電子透かしエンコーダ 3 1 のエンコードの方法に対応したデコード（復号化）処理を行い、指紋画像信号からそこに埋め込まれた透かしデータを分離して検出する。

【 0 0 4 9 】

指紋入力装置 3 は指紋画像信号とは別に、その装置固有の I D（識別子）を指紋照合部 4 に送る。指紋照合部 4 ではその内部の指紋入力装置 I D 保持部 4 3 に、その指紋照合部 4 が接続して使用する指紋入力装置 3 の個体に対応する秘密情報をその入力装置の識別子（装置 I D）と対にして記憶しておく。この秘密情報は該当指紋入力装置の指紋入力装置秘密情報保持部 3 3 に保持されている情報と同一のものである。

【 0 0 5 0 】

指紋入力装置 I D 保持部 4 3 は指紋入力装置 3 から受取った I D でこのテーブルをひき、対応する秘密情報を読み出して指紋入力装置 I D 比較部 4 4 に渡す。指紋入力装置 I D 比較部 4 4 はその値と、電子透かしデコーダ 4 2 において検出された透かしデータとを比較する。もしも、指紋入力装置 3 が正当なものであればこれらは一致するはずであり、そうでなければ不一致となる。

【 0 0 5 1 】

指紋特徴抽出部 2 2 は電子透かしデコーダ 4 2 から出力された画像情報から指紋照合に用いる特徴を計算する。ユーザ別指紋登録情報テーブル 2 6 は指紋照合に用いる指紋特徴情報をユーザ毎に保持しているものである。指紋特徴照合部 2 3 は指紋特徴抽出部 2 2 で求められた指紋特徴とユーザ別指紋登録情報テーブル 2 6 に登録された指紋特徴との照合を行い、結果を照合結果判定部 2 5 に渡す。

【 0 0 5 2 】

照合結果判定部 2 5 は指紋入力装置 I D 比較部 4 4 が判定する指紋入力装置 3 の正当性と、指紋特徴照合部 2 3 で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。先に述べたように、指紋照合部 4 は使用されているはずの指紋入力装置 3 に固有で秘密であるはずの情報が電子透かしとして埋め込まれていれば、指紋入力装置 3 が正当なもので、また指紋入力装置 3 からの信号が途中で改変されていないことを確認することができたとして、指紋照合結果を信頼できるものであると判断する。

【 0 0 5 3 】

そうでない場合には、それは指紋入力装置 3 が正当なものではないか、または指紋入力装置 3 からの信号が途中で改変されたことを意味するので、指紋照合結

果を信頼できるものではないと判断することになる。

【 0 0 5 4 】

図 3 は本発明の別の実施例による画像入力装置の構成を示すブロック図である。図 3 においては本発明の他の実施例による画像入力装置をネットワークで結ばれた指紋照合に拡張したものである。

【 0 0 5 5 】

指紋入力装置 5 はユーザが利用するサービスクライアント 7 に接続されている。これは例えばユーザのオフィスの机の上にある P C、ユーザの家庭にある P C、あるいは店舗の店頭等にある公衆向けの P O S (P o i n t O f S a l e s) 端末でもよい。これらのサービスクライアントは顧客であるユーザに対してさまざまな情報サービスや電子商取引の提供端末として働くが、ユーザの本人確認・認証に関しては指紋サーバ 6 と指紋入力装置 5 との通信を、中身を変えずに橋渡しする透明な仲介者として機能する。

【 0 0 5 6 】

サービスクライアント 7 に接続された指紋入力装置 5 は本発明の他の実施例と同様の構成を持ち、同様の動作を行う。電子透かしが埋め込まれた指紋入力画像はサービスクライアント 7 を通過して指紋サーバ 6 に送られる。

【 0 0 5 7 】

サービスクライアント 7 とネットワークによって結ばれた指紋サーバ 6 は基本的に本発明の他の実施例と同様の構成を持ち、同様の動作を行う。すなわち、電子透かしを検出し、これによって判定される指紋入力装置 5 の正当性と、指紋特徴照合部 2 3 で求められる指紋照合の結果とを総合し、本人確認の結果として出力する。

【 0 0 5 8 】

但し、指紋入力装置 5 は、本発明の他の実施例の場合と異なり、指紋画像信号とは別に指紋入力装置秘密情報保持部 3 3 に保持された秘密情報を、公開鍵暗号部 5 1 が指紋サーバ 6 に対応する R S A 方式の公開鍵を用いて暗号化して指紋サーバ 6 に送る。

【 0 0 5 9 】

秘密鍵復号部 6 1 では送られてきた信号を自分の公開鍵に対応した秘密鍵によって復号し、指紋入力装置 I D 比較部 4 4 での比較に用いる。指紋サーバ 6 に対応する R S A 方式の公開鍵を用いて暗号化された秘密情報は、その公開鍵に対応した秘密鍵によってのみ復号可能である。

【 0 0 6 0 】

この部分については本発明の他の実施例に準じて、ネットワーク内に結ばれた全ての指紋入力装置 5 に対応する秘密情報と指紋入力装置 5 との対を予め指紋サーバ 6 がその内部に保持しておくという実現法もちろん可能ではあるが、指紋入力装置 5 の数が多くなり、また変更・交換等に対応するためには、このように別のチャンネルで直接秘密情報を送る方が優れているといえる。

【 0 0 6 1 】

指紋サーバ 6 は照合結果判定部 2 5 の出力をサービスクライアント 7 に知らせ、指紋を入力したユーザが正規のユーザでありかつ指紋入力装置 5 が正規の装置であると判定の結果から確認できた時に限り、サービスクライアント 7 はユーザの要求するサービスをそのユーザに対して提供する。

【 0 0 6 2 】

上記の本発明の実施例の説明では、バイオメトリクスの一例として指紋の場合を挙げて説明しているが、指紋センサ 1 1 と、指紋特徴抽出部 2 2、指紋特徴照合部 2 3 の部分を別のバイオメトリクスを入力し、特徴を抽出して照合する手段で置換すれば、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋等の他のバイオメトリクスを使用することも可能である。例えば、声紋の場合にはマイクで入力され、デジタル化された後の音声データに対してマイクと不可分な装置で暗号化や電子透かしの埋め込みを施すことで、入力部の正当性を確認することができる。

【 0 0 6 3 】

このように、照合装置以外は解読できない信号、あるいはその中に埋め込まれた電子透かしを解読し、また改変できない信号をバイオメトリクス入力装置と照合装置との間での通信に用いることによって、バイオメトリクス入力装置が改造、置換されず正当なものであることを判定して本人認証を実行することができる

【 0 0 6 4 】

これによって、バイオメトリクス入力装置が照合装置とケーブルやネットワーク等で接続され、分離している場合でも、ケーブルを付け替えて他の情報機器を結び、他の機会に入手した他人の指紋の画像データを、入力センサを装って照合処理部に入力するという種類のセキュリティアタックを防ぐことができる。つまり、照合処理部ではサービスを要求する本人の指紋と考えてサービスを許可するが、実際は他人の指紋であったということは起こり得ない。

【 0 0 6 5 】

すなわち、データが登録されていない不適合スキャナからの指紋データで置き換えられた場合、データの一部に操作が加えられた場合、一部が失われた場合にはそれらを検知し、認証結果に反映させることができる。

【 0 0 6 6 】

また、本発明の別の実施例の構成をとることによって、ネットワーク上に多数のバイオメトリクス入力装置がある場合にも、それぞれが正当なものであることを確認しながらユーザ認証を実現することができる。

【 0 0 6 7 】

【発明の効果】

以上説明したように本発明によれば、個人に固有の生体特徴であるバイオメトリクスをデジタル化し、そのデジタル化したバイオメトリクスを予め設定された秘密情報である暗号化鍵に基づいて暗号化して出力することによって、バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことができるという効果がある。

【図面の簡単な説明】

【図 1】

本発明の一実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【図 2】

本発明の他の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【図 3】

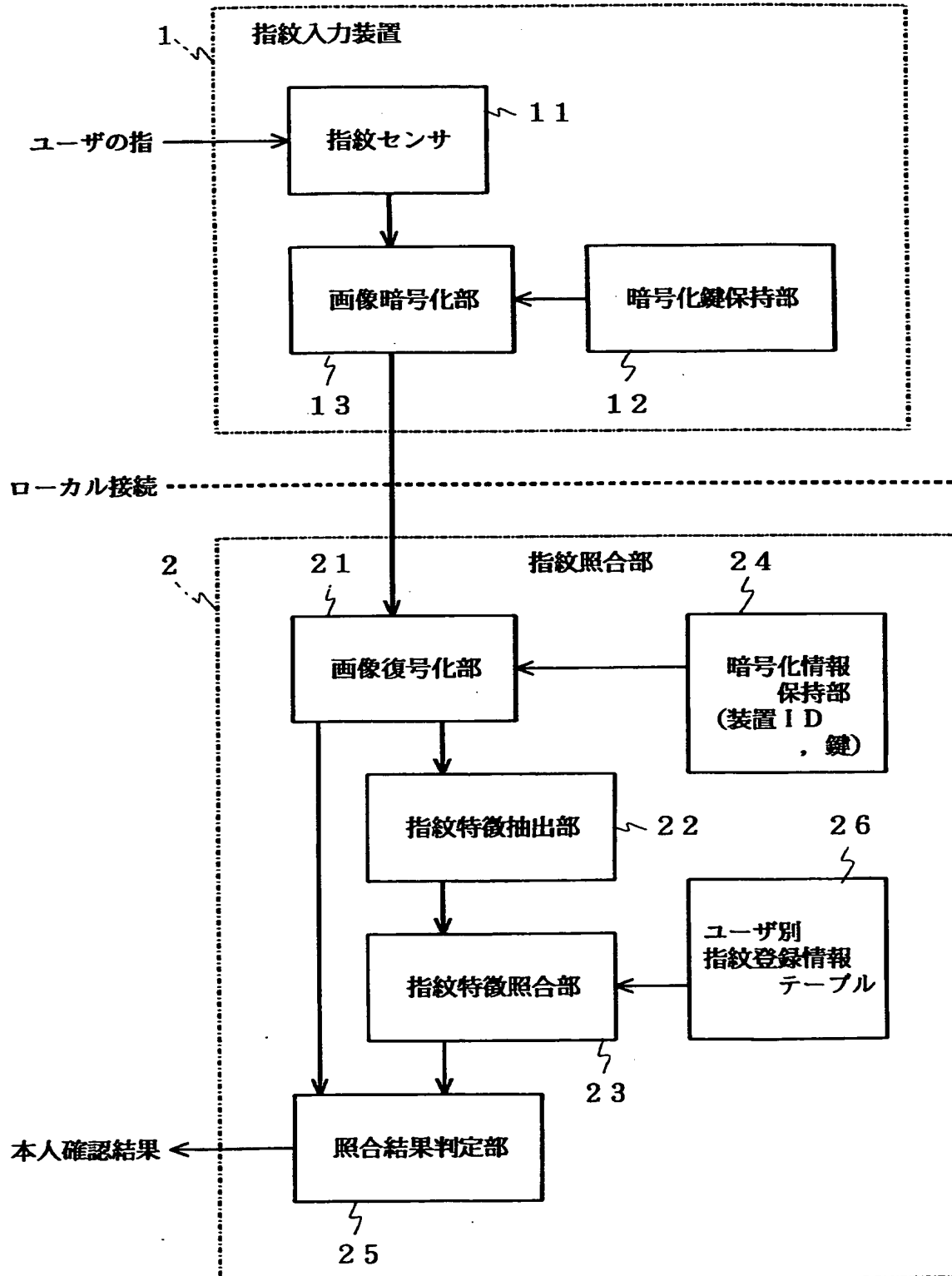
本発明の別の実施例によるバイオメトリクス入力装置の構成を示すブロック図である。

【符号の説明】

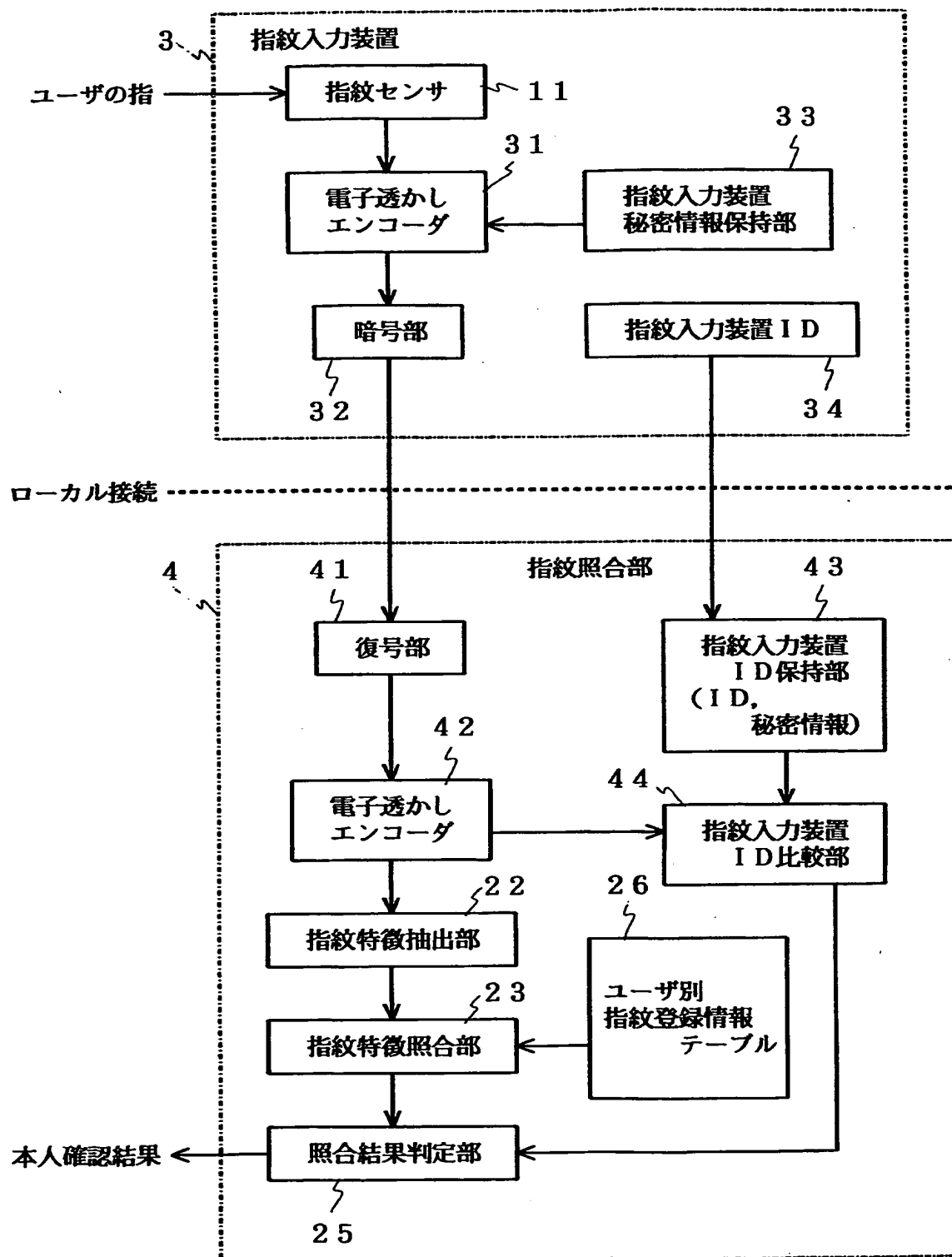
- 1, 3, 5 指紋入力装置
- 2, 4 指紋照合部
- 6 指紋サーバ
- 7 サービスクライアント
- 11 指紋センサ
- 12 暗号化鍵保持部
- 13 画像暗号化部
- 21 画像復号化部
- 22 指紋特徴抽出部
- 23 指紋特徴照合部
- 24 暗号化情報保持部
- 25 照合結果判定部
- 26 ユーザ別指紋登録情報テーブル
- 31 電子透かしエンコーダ
- 32 暗号部
- 33 指紋入力装置秘密情報保持部
- 41 復号部
- 42 電子透かしデコーダ
- 43 指紋入力装置 ID 保持部
- 44 指紋入力装置 ID 比較部
- 51 公開鍵暗号部
- 61 秘密鍵復号部

【書類名】 図面

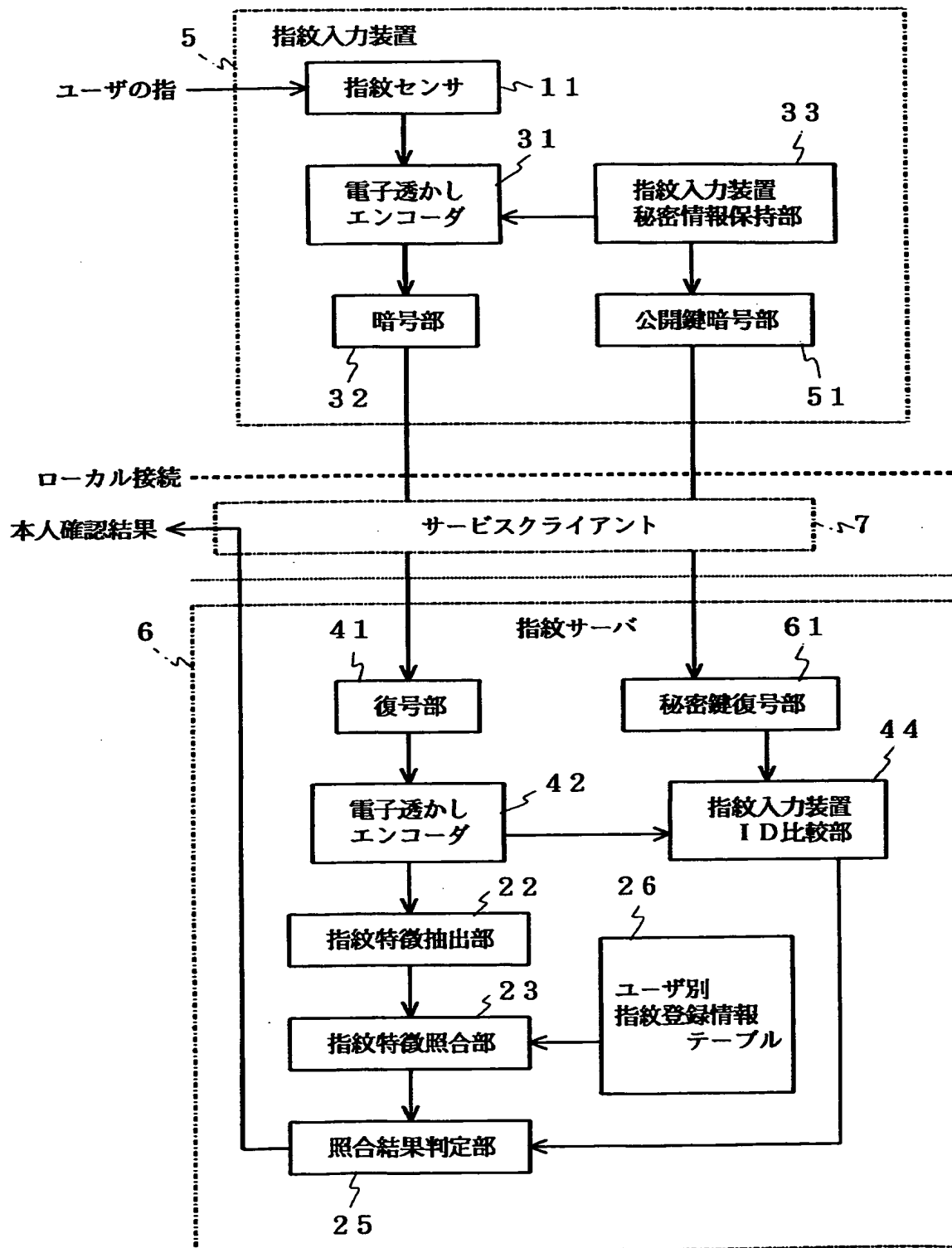
【図 1】



【図2】



【図 3】



【書類名】 要約書

【要約】

【課題】 バイオメトリクス入力部と処理部とが必ずしも一体化していない場合でもセキュリティホールを生じさせることなく、確実な本人確認を行うことが可能なバイオメトリクス入力装置を提供する。

【解決手段】 指紋センサ 1 1 は指が接触した際にその指紋画像を撮影し、撮影した入力画像をデジタルデータに変換してから画像暗号化部 1 3 に送る。画像暗号化部 1 3 は暗号化鍵保持部 1 2 から暗号化鍵を基に入力画像の暗号化処理を行う。画像復号化部 2 1 は暗号化情報保持部 2 4 からの鍵を用い、指紋入力装置 1 から受取った信号を復号する。指紋特徴抽出部 2 2 は復号された結果の画像情報から指紋照合に用いる特徴を計算する。指紋特徴照合部 2 3 は指紋特徴抽出部 2 2 で求められた指紋特徴とユーザ別指紋登録情報テーブル 2 6 に登録されているユーザの指紋特徴との照合を行い、結果を照合結果判定部 2 5 に渡す。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社